The Comprehensive National Cybersecurity Initiative

President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter. Shortly after taking office, the President therefore ordered a thorough review of federal efforts to defend the US information and communications infrastructure and the development of a comprehensive approach to securing America's digital infrastructure.

In May 2009, the President accepted the recommendations of the resulting Cyberspace Policy Review, including the selection of an Executive Branch Cybersecurity Coordinator who will have regular access to the President. He also directed that the Executive Branch work closely with all key players in US cyber security, including state and local governments and the private sector, to ensure an organized and unified response to future cyber incidents; strengthen public/private partnerships to find technology solutions that ensure US security and prosperity; invest in the cutting-edge research and development necessary for the innovation and discovery to meet the digital challenges of our time; and begin a campaign to promote cyber security awareness and digital literacy from our boardrooms to our classrooms and begin to build the digital workforce of the 21st century. Finally, the President directed that these activities be conducted in a way consistent with ensuring the privacy rights and civil liberties guaranteed in the Constitution and cherished by all Americans.

The activities under way to implement the recommendations of this Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) in January 2008. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national US cybersecurity strategy. These CNCI initiatives will play a key role in supporting the achievement of many of the key recommendations of President Obama's Cyberspace Policy Review.

The CNCI consists of a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace:

- **To establish a front line of defense against today's immediate threats** by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.
- **To defend against the full spectrum of threats** by enhancing US counterintelligence capabilities and increasing the security of the supply chain for key information technologies.
- **To strengthen the future cybersecurity environment** by expanding cyber education; coordinating and redirecting research and development efforts across the Federal government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

In building the plans for the CNCI, it was quickly realized that these goals could not be achieved without also strengthening certain key strategic foundational capabilities within the Government. Therefore, the CNCI includes funding within the federal law enforcement, intelligence, and defense communities to enhance such key functions as criminal investigation; intelligence collection, processing, and analysis; and information assurance critical to enabling national cyber security efforts.

The CNCI was developed with great care and attention to privacy and civil liberties concerns in close consultation with privacy experts across the government. Protecting civil liberties and privacy rights remain fundamental objectives in the implementation of the CNCI.

In accord with President Obama's declared intent to make transparency a touchstone of his presidency, the Cyberspace Policy Review identified enhanced information sharing as a key component of effective cybersecurity. To improve public understanding of Federal efforts, the Cybersecurity Coordinator has directed the release of the following summary description of the CNCI.

CNCI Initiative Details

Initiative #1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections. The Trusted Internet Connections (TIC) initiative, headed by the Office of Management and Budget and the Department of Homeland Security, covers the consolidation of the Federal Government's external access points (including those to the Internet). This consolidation will result in a common security solution which includes: facilitating the reduction of external access points, establishing baseline security capabilities; and, validating agency adherence to those security capabilities. Agencies participate in the TIC initiative either as TIC Access Providers (a limited number of agencies that operate their own capabilities) or by contracting with commercial Managed Trusted IP Service (MTIPS) providers through the GSA-managed NETWORX contract vehicle.

Initiative #2. Deploy an intrusion detection system of sensors across the Federal enterprise. Intrusion Detection Systems using passive sensors form a vital part of US Government network defenses by identifying when unauthorized users attempt to gain access to those networks. DHS is deploying, as part of its EINSTEIN 2 activities, signature-based sensors capable of inspecting Internet traffic entering Federal systems for unauthorized accesses and malicious content. The EINSTEIN 2 capability enables analysis of network flow information to identify potential malicious activity while conducting automatic full packet inspection of traffic entering or exiting US Government networks for malicious activity using signature-based intrusion detection technology. Associated with this investment in technology is a parallel investment in manpower with the expertise required to accomplish DHS's expanded network security mission. EINSTEIN 2 is capable of alerting US-CERT in real time to the presence of malicious or potentially harmful activity in federal network traffic and provides correlation and visualization of the derived data. Due to the capabilities within EINSTEIN 2, US-CERT analysts have a greatly improved understanding of the network environment and an increased ability to address the weaknesses and vulnerabilities in Federal network security. As a result, US-CERT has greater situational awareness and can more effectively develop and more readily share security relevant information with network defenders across the US Government, as well as with security professionals in the private sector and the American public. The Department of Homeland Security's Privacy Office has conducted and published a Privacy Impact Assessment for the EINSTEIN 2 program.

Initiative #3. Pursue deployment of intrusion prevention systems across the Federal enterprise. This Initiative represents the next evolution of protection for civilian Departments and Agencies of the Federal Executive Branch. This approach, called EINSTEIN 3, will draw on commercial technology and specialized government technology to conduct real-time full packet inspection and threat-based decision-making on network traffic entering or leaving these Executive Branch networks. The goal of EINSTEIN 3 is to identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response. It will have the ability to automatically detect and respond appropriately to cyber threats before harm is done, providing an intrusion prevention

system supporting dynamic defense. EINSTEIN 3 will assist DHS US-CERT in defending, protecting and reducing vulnerabilities on Federal Executive Branch networks and systems. The EINSTEIN 3 system will also support enhanced information sharing by US-CERT with Federal Departments and Agencies by giving DHS the ability to automate alerting of detected network intrusion attempts and, when deemed necessary by DHS, to send alerts that do not contain the content of communications to the National Security Agency (NSA) so that DHS efforts may be supported by NSA exercising its lawfully authorized missions. This initiative makes substantial and long-term investments to increase national intelligence capabilities to discover critical information about foreign cyber threats and use this insight to inform EINSTEIN 3 systems in real time. DHS will be able to adapt threat signatures determined by NSA in the course of its foreign intelligence and DoD information assurance missions for use in the EINSTEIN 3 system in support of DHS's federal system security mission. Information sharing on cyber intrusions will be conducted in accordance with the laws and oversight for activities related to homeland security, intelligence, and defense in order to protect the privacy and rights of U.S. citizens.

- DHS is currently conducting a exercise to pilot the EINSTEIN 3 capabilities described in this initiative based on technology developed by NSA and to solidify processes for managing and protecting information gleaned from observed cyber intrusions against civilian Executive Branch systems. Government civil liberties and privacy officials are working closely with DHS and US-CERT to build appropriate and necessary privacy protections into the design and operational deployment of EINSTEIN 3.

Initiative #4: Coordinate and redirect research and development (R&D) efforts. No single individual or organization is aware of all of the cyber-related R&D activities being funded by the Government. This initiative is developing strategies and structures for coordinating all cyber R&D sponsored or conducted by the US government, both classified and unclassified, and to redirect that R&D where needed. This Initiative is critical to eliminate redundancies in federally funded cyber security research, and to identify research gaps, prioritize R&D efforts, and ensure the taxpayers are getting full value for their money as we shape our strategic investments.

Initiative #5. Connect current cyber ops centers to enhance situational awareness. There is a pressing need to ensure that government information security offices and strategic operations centers share data regarding malicious activities against federal systems, consistent with privacy protections for personally identifiable and other protected information and as legally appropriate, in order to have a better understanding of the entire threat to government systems and to take maximum advantage of each organization's unique capabilities to produce the best overall national cyber defense possible. This initiative provides the key means necessary to enable and support shared situational awareness and collaboration across six centers that are responsible for carrying out US cyber activities. This effort focuses on key aspects necessary to enable practical mission bridging across the elements of U.S. cyber activities: foundational capabilities and investments such as upgraded infrastructure, increased bandwidth, and integrated operational capabilities; enhanced collaboration, including common technology, tools, and procedures; and enhanced shared situational awareness through shared analytic and collaborative technologies.

- The National Cybersecurity Center (NCSC) within the Department of Homeland Security will play a key role in securing US Government networks and systems under this initiative by coordinating and integrating information from the six centers to provide cross-domain situational awareness, analyzing and reporting on the state of US networks and systems, and fostering interagency collaboration and coordination.

Initiative #6. Develop and implement a government-wide cyber counterintelligence (CI) plan. A government-wide cyber counterintelligence plan is necessary to coordinate activities across all Federal Agencies to detect, deter, and mitigate the foreign-sponsored cyber intelligence threat to U.S. and private sector information systems. To accomplish these goals, the plan establishes and expands cyber CI education and awareness programs and workforce development to integrate CI into all cyber operations and analysis, increase employee awareness of the cyber CI threat, and increase counterintelligence collaboration across the government. The Cyber CI Plan is aligned with the *National Counterintelligence Strategy of the United States of America (2007)* and supports the other programmatic elements of the CNCI.

Initiative #7. Increase the security of our classified networks. Classified networks house the Federal Government's most sensitive information and enable crucial war-fighting, diplomatic, counterterrorism, law enforcement, intelligence, and homeland security operations. Successful penetration or disruption of these networks could cause exceptionally grave damage to our national security. We need to exercise due diligence in ensuring the integrity of these networks and the data they contain.

Initiative #8. Expand cyber education. While billions of dollars are being spent on new technologies to secure the US Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts within the Federal government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cyber security, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge.

Initiative #9. Define and develop enduring "leap-ahead" technology, strategies, and programs. One goal of the CNCI is to develop technologies that provide increases in cyber security by orders of magnitude above current systems and which can be deployed within 5 to 10 years. This initiative seeks to develop strategies and programs to enhance the component of the government R&D portfolio that pursues high-risk/high-payoff solutions to critical cyber security problems. The Federal Government has begun to outline Grand Challenges for the research community to help solve these difficult problems that require 'out of the box' thinking. In dealing with the private sector, the government is identifying and communicating common needs that should drive mutual investment in key research areas.

Initiative #10. Define and develop enduring deterrence strategies and programs. Our Nation's senior policymakers must think through the long-range strategic options available to the United States in a world that depends on assuring the use of cyberspace. To date, the U.S. Government has been implementing traditional approaches to the cybersecurity problem—and these measures have not achieved the level of security needed. This Initiative is aimed at building an approach to cyber defense strategy that deters interference and attack in cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses by both state and non-state actors.

Initiative #11. Develop a multi-pronged approach for global supply chain risk management. Globalization of the commercial information and communications technology marketplace provides increased opportunities for those intent on harming the U.S. by penetrating the supply chain to gain

unauthorized access to data, alter data, or interrupt communications. Risks stemming from both the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services. Managing this risk will require a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and partnership with industry to develop and adopt supply chain and risk management standards and best practices. This initiative will enhance Federal government skills, policies, and processes to provide departments and agencies with a robust toolset to better manage and mitigate supply chain risk at levels commensurate with the criticality of, and risks to, their systems and networks**.**

Initiative #12. Define the Federal role for extending cybersecurity into critical infrastructure domains. The US Government depends on a variety of privately owned and operated critical infrastructures to carry out the public's business. In turn, these critical infrastructures rely on the efficient operation of information systems and networks that are vulnerable to malicious cyber threats. This Initiative builds on the existing and ongoing partnership between the Federal Government and the public and private sector owners and operators of Critical Infrastructure and Key Resources (CIKR). The Department of Homeland Security and its private-sector partners have developed a plan of shared action with an aggressive series of milestones and activities. It includes both short-term and long-term recommendations, specifically incorporating and leveraging previous accomplishments and activities that are already underway. It addresses security and information assurance efforts across the cyber infrastructure to increase resiliency and operational capabilities throughout the CIKR sectors. It includes a focus on public-private sharing of information regarding cyber threats and incidents in both government and CIKR